U.S. House of Representatives

Committee on Ways and Means
Subcommittee on Social Security

Statement for the Record

Hearing on the Role of Social Security Numbers in Identity Theft and Options to Guard Their Privacy

The Honorable Patrick P. O'Carroll, Jr.
Inspector General
Social Security Administration

April 13, 2011

Good afternoon, Chairman Johnson, Mr. Becerra, and members of the Subcommittee. As always, it's a pleasure to appear before you, and I thank you for the invitation to testify today. I have appeared before this Subcommittee many times to discuss issues critical to the Social Security Administration (SSA) and the services the Agency provides to American citizens. Today, we are discussing the Social Security number (SSN) and ways to improve SSN protection and guard against misuse and identity theft.

I last spoke to the Subcommittee about this issue in June 2007, but with SSN use widespread throughout government programs and financial transactions, and technology constantly evolving, the threat of SSN misuse and identity theft lingers. We in the Office of the Inspector General (OIG) are well aware of the central role that the SSN plays in American society, and part of our mission is to protect its integrity along with the other personally identifiable information (PII) within Social Security Administration (SSA) records. To provide some context on the issue, in Fiscal Year (FY) 2009, SSA processed about 6 million original SSN cards and 12 million replacement SSN cards; and received about $671 billion in employment taxes related to earnings under assigned SSNs. Protecting the SSN and properly posting wages under SSNs is paramount to ensuring SSN integrity and protecting our citizens' PII.

As the Subcommittee is well aware, the SSN was created in 1935 to keep an accurate record of each person's Social Security earnings, but over the years, Federal and State governments have relied on the SSN as the identifier of choice for a variety of government programs. Financial institutions are also required to obtain the SSNs of their customers. With each new use, the SSN has more value, and when you create something of value, someone will try to steal it. In May 2006, President Bush ordered the establishment of the National Identity Theft Task Force, which created directives for Federal agencies to strengthen efforts to protect against identity theft. Our reviews have found that SSA has followed these directives for years and strives to improve SSN integrity.

SSA has implemented numerous improvements in its SSN assignment, or enumeration, process. We believe SSA's improved procedures have reduced its risk of improperly assigning these important numbers. Some of the Agency's more notable improvements include:

- establishing enumeration centers that focus exclusively on assigning and issuing SSN cards;
- requiring that field office personnel who process SSN applications use a standardized Web-based, intranet process known as SSNAP, which reinforces Agency enumeration policies and standardizes data collection; and
- strengthening the requirements for identity documents presented with SSN applications to ensure that the correct individual obtains the correct SSN.

In addition, to prevent misuse of personal information, SSA has reported the following actions:

- SSA removed SSNs from the Social Security Statement, displaying only the last four digits.
- The Department of the Treasury removed the SSN and other types of numeric identifiers from Federal checks.
- SSA no longer releases SSNs or any PII to a caller who cannot provide his or her SSN. SSA now refers such callers to field offices for further verification of their identity before releasing any information.
- When SSA assigns a new SSN because a person has recently been disadvantaged by the misuse of his or her SSN, a special indicator is placed on the old SSN record to block issuance of replacement SSN cards and SSN printouts.

Several years ago, to keep track of OIG's many efforts to protect the SSN, we formed the Social Security Number Integrity Protection Team, or SSNIPT. That group, comprised of attorneys, auditors, and investigators, led to the eradication of displays of SSNs on Selective Service mailings and the Thrift Savings Plan Website—two practices by which the Federal government was itself putting the SSN at risk. We are very pleased to learn that the Department of Defense is replacing the SSN with a DOD identification number on all agency identification cards, to protect the privacy and personal information of our military personnel.

We applaud these and other efforts, but even now, SSA has no authority to prohibit the legitimate collection and use of SSNs. Moreover, our audit and investigative work has taught us that the more SSNs are unnecessarily used, the higher the probability that these numbers can be used to facilitate the commission of crimes throughout society. We believe SSA should support legislation to limit public and private entities' collection and use of SSNs, and improve the protection of the information when obtained; continue its efforts to safeguard and protect PII; and develop appropriate authentication measures to ensure the highest level of security and identity assurance before offering replacement SSN cards over the Internet.

Our ongoing and recently completed audit work has highlighted vulnerabilities and suggested some ways in which SSA can persuade public and private organizations to limit the collection, use, and disclosure of SSNs. We are working on or have completed the following related reviews:

- We are currently conducting an audit to assess State Departments of Health use of SSNs in their newborn screening process. Our focus will be to determine whether States have adequate controls in place to safeguard SSNs.

- *Kindergarten Through 12th Grade Schools' Collection and Use of SSNs*, released in July 2010, determined that many K-12 schools used SSNs as the primary identifier for students or for other purposes, even when another identifier would have sufficed. We believe that while some schools use SSNs as a matter of convenience, administrative convenience should never be more important than safeguarding children's personal information.

- *Prisoners' Access to SSNs*, released in March 2010, was a follow-up to a 2006 review that found that prisons in 13 States allowed inmates access to SSNs through various work programs. We determined that eight of the 13 States identified in our 2006 report continued this practice. However, in December 2010, the President signed the *Social Security Number Protection Act of 2010*, which prohibited prison work programs from granting prisoners access to SSNs.

- *State and Local Governments' Collection and Use of SSNs*, released in September 2007, identified instances in which some State and local governments posted public documents that contained SSNs on the Internet. We recommended that SSA seek legislation to limit SSN collection by State and local governments.

Although temporary residents may have authorization to work in the United States for the limited time they are here, we question the propriety of assigning an SSN, which is valid for life, to these individuals, because the SSN may be a key to a temporary resident's ability to overstay his or her visa. We are working on or have completed the following related reviews:

- Because of numerous instances of fraud and abuse in the H1-B (non-immigrant) worker program, we are currently conducting an audit to assess these workers' use of SSNs. An individual in the H1-B visa program is allowed to work for only one specific employer that has been approved by the Departments of Labor and Homeland Security. Our focus will be to determine whether these non-immigrants are working for their approved employers.

- *Assignment of SSNs to Noncitizens with Fiancé Visas*, released in May 2008, questioned the approval of an SSN to someone for as long as three months before they marry, because SSA might be giving those who have no intention to marry a tool for overstaying their visas. We recommended that SSA discuss with the Department of Homeland Security the feasibility of not granting work authorization to K-1 visa holders until they marry, but SSA and DHS determined it was not feasible.

- *Assignment of SSNs to J-1 Exchange Visitors*, released in July 2007, recommended that SSA work with the IRS to develop alternatives to assigning SSNs to certain types of exchange visitors, including the IRS' issuing Individual Taxpayer Identification Numbers. SSA declined to do so, stating that changing the way individuals are enumerated under the two J-1 categories we reviewed would create inconsistencies with policies regulating the other 11 categories.

Another issue to consider is SSA's procedures for issuing SSN Verification Printouts. Under the *Privacy Act*, individuals are allowed to obtain their SSN information from SSA, and the printout is among the items available. The printout is a limited version of the Numident record, but it still contains the same basic information as the Social Security card. The printout, however, has no security features.

SSA's current disclosure regulations that implement the *Privacy Act* allow an individual to provide less probative identity documents to obtain an SSN Printout. In certain circumstances, an individual can obtain the SSN printout from a field office without any identity documents. In a December 2007 report, *Controls for Issuing Social Security Number Verification Printouts*, we said procedures for issuing the printouts should follow SSA's improved replacement card procedures.

In response to the *Intelligence Reform and Terrorism Prevention Act of 2004*, SSA revised its policies and procedures for issuing Social Security replacement cards. Some of SSA's actions included increasing the identity requirements, such as presenting valid photo identification documents for obtaining a replacement SSN card; and limiting the number of replacement Social Security cards an individual can receive to no more than three in a year and 10 in a lifetime.

However, SSA did not implement similar procedures in the SSN printout issuance process. Our ongoing audit on SSA's controls over the issuance of SSN printouts determined the Agency issued about 7 million printouts in FY 2009, up from about 4.6 million in FY 2003, the first full year SSA issued the printouts. That audit is almost complete, and we anticipate issuing a report early this summer.

Turning to the issue of identity theft, the Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year. The victim and their families often suffer mentally and emotionally as they attempt to repair the cracks in their financial foundation. The Martinez family, unfortunately, has coped with the effects of identity theft for several years, as I will explain.

Dr. Juan Martinez is a 37-year-old assistant professor of microbiology. Dr. Martinez was born and raised in southwest Chicago, so he was thrilled to accept a position teaching at the University of Chicago

in 2005. Shortly thereafter, Dr. Martinez received a letter from the IRS that stated he failed to pay taxes on wages earned the previous year in Colorado; the letter arrived with a substantial bill. Although Dr. Martinez had never worked in Colorado, someone using his name, SSN, and date of birth had received wages there from a facilities management company. Dr. Martinez then had to go about proving his case to the IRS, tracking down credit reports, bank records, and cell phone accounts, all while searching for a person who was working under a common Hispanic name.

Local law enforcement authorities eventually referred the case to one of our investigators, Special Agent Thomas Brady, who has investigated many identify theft cases. Brady worked with Dr. Martinez and Bank of America, where the other "Juan Martinez" had opened an account. Bank of America provided Agent Brady with account records, including a Missouri address and a photo taken at an ATM.

Agent Brady went to the address in Missouri, and the man who answered the door was the man in the ATM photo. He identified himself as Roberto Ramos-Carvente, and he admitted to obtaining false documents and using Dr. Martinez's identity to gain employment at a restaurant, rent his apartment, and open a bank account in Missouri.

Our investigation resulted in criminal charges of SSN misuse and identity theft against Mr. Ramos-Carvente, who was sentenced in March 2011 to seven months in prison and two years' supervised release. He was also ordered to pay restitution of $5,650 to Dr. Martinez. Finally, Ramos-Carvente was ordered to participate in deportation proceedings and remain outside the United States, if deported.

Dr. Martinez is grateful for our efforts in resolving this issue, but a huge amount of credit goes to the victim himself for working tirelessly to track down the person who had stolen his identity. Nevertheless, we are very pleased to have helped Dr. Martinez, and while he could not be here today, he has prepared a written statement for the record. He has said he wants to help others protect themselves so they can avoid the trauma of identity theft.

As we pursue investigations similar to the case of Dr. Martinez, our agents also participate on about 45 SSN misuse task forces throughout the country, which cover mortgage fraud, bankruptcy fraud, and document and benefit fraud, as well as identity theft. In FY 2010, we opened 309 cases related to SSN misuse, which accounted for about 5 percent of all cases we opened during that period. In addition, in FY 2010, we had 441 SSN misuse cases that resulted in a criminal conviction, as a result of either a sentencing or a pre-trial diversion.

We support the prior bipartisan legislative efforts of this Subcommittee to limit the use, access, and display of the SSN in the public and private sectors; and to increase penalties against those who fraudulently misuse the SSN. Most recently, the Subcommittee introduced the *Social Security Number Privacy and Identity Theft Prevention Act of 2009*. This legislation included new criminal penalties for the misuse of SSNs; criminal penalties for SSA employees who knowingly and fraudulently issue Social Security cards or SSNs; and enhanced penalties in cases of terrorism, drug trafficking, crimes of violence, or prior offenses.

The legislation would also expand the types of activities that are subject to civil monetary penalties (CMP) and assessments under Section 1129 of the *Social Security Act*. Currently, an individual who misuses an SSN is not subject to a CMP, except in cases related to the receipt of Social Security benefits or Supplement Security Income. The legislation would authorize the imposition of CMPs and

assessments for activities such as providing false information to obtain an SSN, using an SSN obtained through false information, or counterfeiting an SSN.

The expanded use of the SSN in today's society has made it a valuable commodity for criminals. In addition to being a lynchpin for identity theft crimes, it also assists an individual to assimilate into our society, in some instances to avoid detection. The importance of SSN integrity to prevent identity theft and ensure homeland security is universally recognized. Providing enhanced, structured penalties is appropriate to reflect the vital importance of the SSN.

As we saw with Dr. Martinez, identity theft can take many forms, as an individual used his SSN to gain employment, rent an apartment, and open bank accounts. Identity theft is serious, and while OIG and SSA have controls in place to protect the SSN, we should all be aware of the dangers of being careless with our personal information. We urge people to keep their Social Security cards in a secure place, to shred personal documents, and to be aware of phishing scams, because no reputable financial institution or company will ask for personal information like an SSN via the Internet. It is also important to protect personal computers with a firewall and updated anti-virus protection.

Additionally, we should all be judicious in giving out an SSN in business transactions, because while it is required for financial transactions, an SSN is not necessary for everyday transactions like applying for a gym membership. It is also critically important that we all monitor our financial information regularly by checking credits report from one of the three major credit bureaus. By knowing how to protect ourselves, we can make life much more difficult for identity thieves.

In conclusion, SSA has a long history of protecting PII, and while current conditions may be the most challenging yet, we are confident SSA will rise to the occasion and address the challenges of today and tomorrow. Identity theft will undoubtedly persist for years to come, because of the reliance on the SSN as a national identifier and advances in technology and communication, but we are committed to ensuring that the information in SSA's records remains safe and secure. The SSN was never intended to do more than track a worker's earnings and to pay that worker benefits, but as the use of the SSN has expanded over the decades, its value has increased as a tool for criminals. Therefore, we must continue to ensure the integrity of the enumeration process; limit the collection, use, and public display of the SSN; encourage the protection of the SSN by those who use it legitimately; and provide meaningful sanctions for those who fail to protect the SSN or misuse it.

The OIG has done, and continues to do, significant audit and investigative work related to SSN misuse and identity theft. We will continue to provide information to Agency decision-makers and this Subcommittee about this critically important issue. I thank you again for the invitation to speak with you today, and I'd be happy to answer any questions.

Chairman JOHNSON. Thank you. I am told that most of the stolen numbers are from young people who have not yet begun to work. Is that your information?

Mr. O'CARROLL. I would qualify that by saying that a lot of them belong to children that haven't begun to work. And when people are vacuuming up numbers that are out there, often times they are targeting children's numbers. But I cannot say it is exclusive.

Chairman JOHNSON. That is because they have not ever recorded them anywhere.

Mr. O'CARROLL. Agreed.